REMARKS

Claims 1, 3-7, 11-12, 16-17, 19-20, 22-26, 28, 30-31, 35-36, 38-39, 41-45, 47, 49-50, 54-55, 57-62, 64 and 67-70 are pending with claims 1, 20, and 39 being independent.

Claims 1, 3-7, 11-12, 16-17, 19-20, 22-26, 28, 30-31, 38-39, 41-45, 47, 49-50, 54-55, 57-62, 64 and 68-70 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Cox (U.S. 6,738,814) in view of Eichstaedt et al. (U.S. 6,662,230) and in further view of Maher, III et al. (U. S. 6,654,373), in further view of Alcendor (U. S. 6,337,899). Applicants respectfully traverse, pointing out below the reasons for traversal first with reference to independent claim 1 and then with other claims.

As amended, claim 1 recites a method for securing an accessible computer system, the method includes, receiving more than one data packet at a network device, each data packet including a payload portion and an attribute portion and being communicated between at least one access requestor and at least one access provider through the network device, monitoring, at the network device, at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors by scanning the payload portion for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern; and using the network device to deny subsequent data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor is deemed to include the predetermined pattern exceed a configurable threshold number.

Applicants respectfully request reconsideration and withdrawal of the rejection because Cox, Eichstaedt, Maher and Alcendor, either alone or combined as proposed, fail to disclose or suggest denying subsequent data packets from access requestors based on the results of monitoring the payload portion of the data packets directed from access providers, as claimed.

The Office Action acknowledges the failure of Cox to teach the feature of denying subsequent data packets from the access requestors based on the results of monitoring the payload portions of data packets directed from the access providers, and the Office Action similarly fails to rely on either of Eichstaedt or Maher for this feature, instead relying exclusively

on Alcendor for the teaching of this feature. However, Alcendor also fails to teach this feature. In fact, Alcendor does not disclose anything that relates to data packets, much less on monitoring the data packets directed from the access providers; consequently, Alcendor has no mention of further denying subsequent data packets from the access requestors.

More particularly, Alcendor merely describes a method of authenticating users in telephony response systems, where users are temporarily inconvenienced to reselect the desired service after a number of failed login attempts, as shown in paragraph 2-3 of column 7 and Fig. 4 of Alcendor. Alcendor only monitors the number of failed login attempts of a user; Alcendor does not monitor the traffic from the access providers. Additionally, nowhere does Alcendor describe or suggest denying subsequent data packets from the access requestors based on the results of monitoring the payload portions of data packets directed from access providers, as claimed. In fact, this deficiency alone makes Alcendor unable to cure Cox's deficiency. Therefore, the proposed combination of Alcendor, Cox, Eichstaedt and Maher is deficient for failure of any of these references to teach or suggest the feature of denying subsequent data packets from the access requestors based on the results of monitoring payload portions of the data packets directed from the access providers.

In the response to the non-final Office action of 02/03/06, Applicant further clarified the distinction from Alcendor by pointing out that Alcendor lacks the use of an intermediary network device, as required by claim 1. Such additional distinction further demonstrates that Alcendor's system has a different structure and solves a different problem. More specifically, all inbound requests of Alcendor reaches the intelligent peripheral system (IP system), which compare to the access provider. Nowhere does Alcendor describe or suggest an intermediary network device that is separate from the IP system, wherein the network device is able to receive the inbound requests and deny their access to the IP system after monitoring feedback from the IP system.

To meet the claimed intermediary network device limitation of claim 1, the Office Action suggests combining Cox's routing device with Alcendor's system and performance of Alcendor's functions on Cox's routing device. However, , there exist no motivation for such a combination, other than the impermissible hind sight gleaned by the present application's teachings. Authenticating users is the main focus of Alcendor's IP system. There is no reason to introduce a separate network device to perform the major function of the IP system disclosed by

Alcendor. Rather, absent impermissible hindsight, one would be led to perform the function using the technology taught by Alcendor, including the architecture taught by Alcendor.

Moreover, if combined as suggested, the main function of Alcendor would be performed at the network device, leaving the main IP system of Alcendor with no use. On the other hand, the structured difference between Alcendor and Cox again emphasized that Alcendar is solving a different problem and has a totally different focus.

Additionally, even if, for the sake of the Office Action, such combination is performed, and assuming Cox's router monitors access providers' responses, it still would not deny traffic from the access requestors. At most, Alcendor solicits additional information from a particular user. Someone trying to thwart high volume attacks by abusive access requestors would not consider such art relevant to a process designed to do deny subsequent communications from abusive requestors.

Accordingly, Alcendor's patent, like Cox, Eichstaedt and Mahet, fails to teach or suggest the feature of monitoring data packets directed from the access providers and denying subsequent data packets from the access requestors, and the feature of performing the monitoring and denying data packets using a network device. Therefore, Alcendor's patent cannot be properly combined with the other references to suggest such features.

For at least these reasons, the proposed combination of Cox, Eichstaedt, Maher and Alcendor fail to teach or suggest the features of "monitoring, at the network device, at least the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors by scanning the payload portion for at least one predetermined pattern and counting a number of data packets having payload portions that include the predetermined pattern; and using the network device to deny subsequent data packets from the access requestor to the access provider.

For at least these reasons, independent claim 1 and its dependant claims are believed to be allowable over the applied combination of references.

Similarly, independent claim 20 recites "..to deny communication of subsequent data packets from the access requestor to the access provider when a number of payload portions of data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number."

Independent claim 39 recites "...to deny communication of subsequent access by data packets from the access requestor to the access provider when a number of payload portions of the data packets received from the access provider to the access requestor that include the predetermined pattern exceed a configurable threshold number."

For at least the similar reasons as stated above, independent claim 20, 39 and their respective dependant claims are believed to be allowable over the applied combination of references.

It is believed that all claims are in condition for allowance, and such action is respectfully requested to the Examiner.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 10/10/2006

W. Karl Renner
Reg. No. 41,265

Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331